Formal Design of Cryptographic Hardware

著者	上野 嶺
号	23
学位授与機関	Tohoku University
学位授与番号	情博第651号
URL	http://hdl.handle.net/10097/00122978

氏名（本籍地）	上野 嶺（うえの れい）
学位の種類	博　士（情報科学）
学位記番号	情　博　第　651　号
学位授与年月日	平成３０年　３月２７日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	Formal Design of Cryptographic Hardware （暗号ハードウェアの形式的設計に関する研究）
論文審査委員	（主査）東北大学教　授　青木　孝文 東北大学教　授　静谷　啓樹　東北大学教　授　張山　昌論 東北大学教　授　本間　尚文 （工学研究科）

論文内容の要旨

第１章　緒言

秘匿通信や認証，電子署名などに基づく安全な情報システムを実現するために暗号技術が用いられている．近年では，暗号技術はスマートカードなどのリソースの制約が厳しい組み込み機器への搭載が進んでおり，暗号演算を効率的に行う暗号ハードウェアが広く普及している．LSI機器の急速な増加に伴い暗号ハードウェアに求められる性能や機能も多様化しているため，高速かつ正確な暗号ハードウェアの設計に高い需要がある．現代暗号のほとんどはガロア体算術と呼ばれる特殊な数体系上の演算により実現されるため，暗号ハードウェアの大部分を構成するガロア体算術演算回路の適切な設計が強く求められている．

その一方で，暗号ハードウェアの設計・検証の困難性が問題となっている．現在の回路設計自動化技術（ハードウェア記述言語を用いた高水準設計手法や自動合成技術）はガロア体算術をサポートしていないため，暗号ハードウェア設計時にはガロア体算術演算回路を低水準な論理式により手設計しなければならず，高いコストがかかっている．加えて，ガロア体算術演算回路の論理構造はワードレベルでの記述のみならず演算ルールを決定する既約多項式やガロア体表現により異なるため，整数環算術を主な対象として発展してきたこれまでの高水準設計手法や自動合成手法を適用することも難しい．さらに，その回路機能検証においても問題がある．暗号ハードウェア中の回路の誤りはセキュリティ上致命的な脆弱性になり得ることが知られており，暗号ハードウェア設計においては完全な機能検証が強く求められる一方，回路の巨大さや論理構造の複雑性を原因として，多様な暗号ハードウェアの完全な機能検証は現実的には不可能とされていた．

本論文では，上記問題を解決するために，多様な暗号ハードウェアの形式的設計手法の理論的基礎の確立とその実証を行う．

第２章　暗号ハードウェアの設計に関する基礎的考察

第２章では，情報セキュリティにおける暗号技術の位置付けや暗号アルゴリズムの実装について概説し，暗号技術とガロア体算術の関わりについて述べる．その上で，既存の算術演算回路の設計・検証手法について考察し，多様な暗号ハードウェアの設計における課題について述べる．

第３章　ガロア体算術演算回路の形式的設計手法

第三章で提案する設計手法では，数系と数式に基づく階層的グラフを用いてガロア体算術演算回路を表現し，回路機能を表す数式の等価性判定により回路機能を形式的に検証する．提案手法はこれまでの設計手法に対し以下の特徴を有している．まず，(i) 冗長表現やパイプライン化に基づく多様かつ実用的なガロア体算術演算回路に適用可能である．さらに，(ii) 階層間の等価性判定に計算機代数に基づく数式評価と数理論理に基づく数式評価を最適に組み合わせることで多様なガロア体算術演算回路を高速に検証可能である．本論文では，多様かつ実用上重要な回路の形式的設計を行うことで提案手法の有効性を確認する．例えば，従来手法では設計・検証が困難とされていた冗長表現に基づく高性能ガロア体乗算器や世界で最も広く用いられる国際標準暗号の一つである AES (Advanced Encryption Standard) の復号ハードウェア，耐タンパー性暗号ハードウェアの完全検証に成功した．

第４章　暗号ハードウェア向け算術演算回路の自動合成

第４章では，上記設計手法に基づくガロア体算術演算回路の自動合成システムを示す．本システムでは，回路仕様を入力として機能や耐タンパー性が保証されたガロア体乗算器の記述を生成する．生成された記述は既存の回路設計自動化ツールで用いることができるため，本システムは提案設計手法と既存の設計手法を融合するものとして位置付けられる．本システムは一万種類を超えるガロア体乗算器の自動合成が可能であり，暗号ハードウェア設計におけるコストの削減に寄与することが期待される．

第５章　高効率 AES 暗号ハードウェアの設計

第５章では提案手法の有用性を実証するため，提案手法を用いた高効率暗号ハードウェアの設計を行う．ガロア体算術演算回路の性能はガロア体の表現手法に大きく依存する．これまでの暗号ハードウェアは単一のガロア体表現しか用いられて来なかったが，本論文で設計するハードウェアでは従来の正規基底表現に加えて二種類の冗長表現を組み合わせて用いる．さらに，演算の圧縮や回路の共有などの最適化技法を駆使することで，設計した AES 暗号ハードウェアは従来手法の約半分の電力/エネルギーで暗号化・復号が可能である．従来の設計手法ではこのような冗長表現に基づく暗号ハードウェアや最適化が適用された暗号ハードウェアの完全検証は困難であるが，提案設計手法を用いることで高性能かつ最先端の暗号ハードウェアも設計・検証が可能となる．

第６章　結言

本論文では，多様な暗号ハードウェアの形式的設計手法の理論的基礎の確立とその実証を目的として，新たな形式的設計手法を提案し，それに基づく算術演算回路の自動合成システムやそれを応用した高効率暗号ハードウェアの設計を示した．今後は，提案設計手法を様々な機能や性能を有する暗号ハードウェア設計に適用することで高効率暗号ハードウェアの開発を行うとともに，提案設計手法の理論的限界の究明を行うことなどを検討している．

論文審査結果の要旨

近年，暗号技術を搭載する機器は著しく増加しており，用途に応じて適切な暗号ハードウェアを設計することが必要になっている．しかし，最近の暗号ハードウェアは，その多くがガロア体上の算術演算回路（ガロア体算術演算回路）を基本として構成されるため，論理回路の設計に基づく従来の設計技術を適用することが困難であった．著者は，多様なガロア体算術演算回路の統一的な設計技術を確立するために，数式を用いたガロア体算術演算回路の形式的設計法および検証法を考案した．また，これを用いたガロア体算術演算回路の自動合成システムを構築するとともに，その応用として具体的な高効率暗号ハードウェアの設計を示した．本論文はこれらの成果をとりまとめたもので，全文６章からなる．

第１章は，緒言である．

第２章では，暗号技術とガロア体算術演算回路の設計法について概説している．また，暗号ハードウェアの設計と検証に関する基礎的考察を与えている．

第３章では，ガロア体算術演算回路の形式的設計法を提案している．ガロア体算術演算回路の機能表明と内部構造を数式で階層的に記述することによって，多様なガロア体算術演算回路を統一的に表現できることを明らかにしている．さらに，その内部構造から得られる連立方程式により機能表明の方程式が導出可能かどうかを，計算機代数と数理論理学的な手法に基づいて判定し，高速に機能検証を行う方法を確立している．これは優れた成果である．

第４章では，第３章で提案した設計法および検証法に基づくガロア体算術演算回路の自動合成システムを構築している．これは，暗号ハードウェアにおいて利用され得る９千種類以上のガロア体乗算回路を，その機能を保証した上で高速に自動合成することができる．これは有用な成果である．

第５章では，第３章で提案した設計法の応用として，高効率な暗号ハードウェアの設計を示している．特に，最も代表的な共通鍵暗号である AES（Advanced Encryption Standard）に着目し，エネルギー効率に優れた高性能な AES 暗号ハードウェアを設計している．性能評価を通して，１回の暗号化処理にかかる消費エネルギーに関して世界最小を達成できることを示している．これは実用上重要な成果である．

第６章は，結言である．

以上，要するに本論文は，数式に基づくガロア体算術演算回路の形式的設計法を提案するとともに，ガロア体算術演算回路の自動合成システムの構築および高効率な暗号ハードウェアの設計を通してその有用性を示したものであり，計算機工学および情報基礎科学の発展に寄与するところが少なくない．

よって，本論文は博士（情報科学）の学位論文として合格と認める．